Contribution ID: **81** Type: **Poster**

Implementation of zero trust security strategy in HEPS scientific computing system

Thursday, 14 March 2024 16:10 (30 minutes)

Traditionally, data centers provide computing services to the outside world, and their security policies are usually separated from the outside world based on firewalls and other security defense boundaries. Users access the data center intranet through VPN, and individuals or endpoints connected through remote methods receive a higher level of trust to use computing services than individuals or endpoints outside the perimeter. But this approach to security design is never ideal. Zero Trust security is based on de-peripheralization and least-privilege access, which protects intranet assets and services from vulnerabilities inherent in the network perimeter and implicit trust architecture. In order to meet the diverse data analysis needs of light source users, the HEPS scientific computing system provides an interactive computing service model for external network users. Users can directly access intranet computing resources through web pages. In this service model, how do we refer to the zero-trust security idea? It has become very urgent to realize the minimum permission access between various services of the computing system and improve the security level of the system environment. Based on the zero-trust security strategy, this paper designs an inter-service communication mechanism based on user identity tokens. During the function call process between different services, service permissions are allocated based on the token user identity to achieve fine-grained management of service permissions and ensure the Cybersecurity of HEPS scientific computing systems.

Significance

References

Experiment context, if any

Primary authors: Mr XU, Jiping (IHEP); HU, Qingbao (IHEP); CHENG, Yaosong (Institute of High Energy Physics Chinese Academy of Sciences, IHEP); LUO, qi (中科院高能物理所计算中心)

Presenter: HU, Qingbao (IHEP)

Session Classification: Poster session with coffee break

Track Classification: Track 2: Data Analysis - Algorithms and Tools